

PLH



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/304,444	05/03/1999	GREGORY BURNS	MS1-301US	9671
22801	7590	01/13/2004	EXAMINER	
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			KLIMACH, PAULA W	
			ART UNIT	PAPER NUMBER
			2135	8
DATE MAILED: 01/13/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/304,444

Applicant(s)

BURNS ET AL.

Examiner

Paula W Klimach

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 02 October 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☐ Claim(s) _____ is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 10/02/03 (Paper No. 6). Original application contained Claims 1-19. Applicant amended Claims 1 and 7. The amendment filed on 10/02/03 have been entered and made of record. The terminal disclaimer filed on 10/02/03 has been entered and made of record. Therefore, presently pending claims are 1-19.

Response to Arguments

Applicant's arguments filed on 10/02/03 have been fully considered but they are not persuasive because of following reasons.

Applicant argued "the recited assembly is not shown in the Mooney reference". This is not found persuasive because the reference used to replace Mooney, Harari discloses a memory device that is protected by a card as shown in the 102 rejection below. The memory and the card are removably connected to the computer as shown in Fig. 1. The smart card alternatively enables access to the user data when present and disables access to the user data when absent (column 13 line 63 to column 14 line 3). The Harari reference discloses a system that includes both memory and a smart card that are two components.

The applicant further argues, "Claim 2 depends from claim 1, and is allowable by virtue of that dependence." However, claim 1 is rejected as shown below and therefore claim 2 is rejected by virtue of the above-mentioned dependency. Further, the memory disclosed by Harari is removably connected to the Host. The combination of the system disclosed by Harari and the profile disclosed by Hayes would save the profile to the removable memory disclosed by Harari.

The applicant further argues, "Claim 11 recites a computer having a memory drive and a card reader." The memory device disclosed by Harari is removable and portable from computer to computer (column 14 lines 20-30). Since the computer must communicate with the memory as disclosed above, it suggests a memory drive. This memory drive is for a portable memory. The Host interfaces with the card, which is embodied in the combination of the mother and daughter card, and as a result suggests that it has a card reader.

The applicant argues further, "Claim 15 recites storing a user profile in memory of a smart card secured profile carrier...neither teaches interfacing the carrier with a computer to enable access to user profile contained within memory within the carrier." Harari discloses a memory system that enables access to data within the memory of the daughter device.

The applicant argues further, "The applicant stresses that accessing memory within the smart card by password (subject matter of Deo)" is not the same as accessing the memory of the memory device contained, in addition to the smart card, within the profile carrier by using a password. That is, the Applicant recites the smart card is used to protect memory of the profile carrier, which is external to the smart card." This is not persuasive. The memory that is protected in the combination as shown below is the memory disclosed by Harari, which is external to the smart card as shown in Fig. 1.

The applicant argues further, "none of the references disclose (1) a portable memory device, which is used in conjunction with (2) a smart card." This is not found persuasive because Harari discloses a memory system that is removable and therefore portable in conjunction with a smart card.

Art Unit: 2131

The applicant argues further, “none of the references disclose reading the access credentials from the smart card to enable access to the user data on the portable memory device.” This is not found persuasive. Harari discloses storing and therefore reading the access credentials from the smart card to enable access to the user data on the portable memory device (column 13 line 63 to column 14 line 30).

The applicant argues further with regards to claim 4-6, 9-10, and 18, “the art of record does not show the use of a profile carrier, having a memory device and a smart card,” Harari shows the system having a memory device and a smart card.

The examiner asserts that the prior art does teach or suggest the subject matter broadly recited in independent Claims 1, 5, 7, 11, 15, 17, 18, and 19. Dependent Claims 2-4, 6, 8-10, 12-14, and 16 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action (Paper No. 8). Accordingly, rejections for claims 1-19 are respectfully maintained.

Double Patenting

A valid terminal disclaimer was entered in the amendment of 10/02/03. Therefore obviating the double patenting rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

Art Unit: 2131

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1, 7 and 17 rejected under 35 U.S.C. 102(e) as being anticipated by Harari et al (5,887,145).

In reference to claims 1 and 7, Harari discloses a profile carrier, removably connectable to a computer (column 6 line 59 to column 7 line 6). The card can be connected to a host CPU as disclosed in (column 6 lines 44-58). Harari also discloses a memory device to store the user data embodied in the memory of the daughter card (column 9 lines 10-30). Harari also discloses a smart card associated with a user that alternately enables access to the user data on the memory device when both the memory device and smart card are interfaced with a common computer and disables access to the user data when one of the memory device or smart card is absent (column 13 line 63 to column 14 line 19).

In reference to claim 17, this claim differs from claim 1 because of storing access credentials on a smart card the access credentials enabling access to the user data stored on the portable memory device (column 13 line 63 to column 14 line 7).

Claim Rejections - 35 USC § 103

Claim 2, 11, 15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harari as applied to claim 1 above, and further in view of Hayes et al (20010011341).

In reference to claim 2, Harari does not expressly disclose a system wherein the memory device stores a user profile that can be used to configure a computer.

Hayes discloses a user profile that is kept in the user's computer and used to configure the user's computer, page 1 paragraph 4.

Art Unit: 2131

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user's profile described by Hayes in memory device disclosed by Harari.

One of ordinary skill in the art would have been motivated to do this because user would be required to identify themselves and, therefore gain access permission or not, Hayes page 2 paragraph 12.

In reference to claim 11, Harari discloses a computer system having a memory drive (column 12 lines 46-50) and a card reader, column 3 lines 48-54. The Harari discloses a system where the host can be a personal computer; the personal computer obviously has memory and memory drive. Harari also discloses an integrated circuit card (smart card) that is associated with the user and that can be interfaced with the computer via the card reader (column 8 lines 24-57). Harari further discloses a memory device being interfaced with the computer via the memory drive (column 7 lines 48-63) and an IC card that enables access to the user data on the memory device, (column 13 line 63 to column 14 line 19).

However, Harari does not disclose a memory device to store the user's profile.

Hayes discloses a user's profile being stored in memory wherein the profile is accessible to configure the computer (page 1 paragraph 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to save the user's profile described by Hayes in the memory device described by Harari.

One of ordinary skill in the art would have been motivated to do this because it is desirable that the user identify themselves before gaining access permission, Hayes page 2 paragraph 12.

In reference to claim 15, Harari discloses a computer system that stores user data in memory that is secured by a smart card selectively enables access to user data in the memory (column 13 line 63 to column 14 line 19).

Harari does not disclose a system for storing a user's profile for configuring the computer.

Hayes discloses a system where the user's profile is stored in memory for access for configuring the computer, page 1 paragraph 4.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user profile, for configuring the computer that was described by Hayes, in the smart card secured memory system, described by Harari.

One of ordinary skill in the art would have been motivated to do this because it is desirable that the user identify themselves before gaining access permission, Hayes page 2 paragraph 12.

In reference to claim 16, Harari and Hayes disclose the computer system as applied to claim 15. Harari further discloses a system where data can be securely transported from one computer to a second computer (column 14 lines 20-30).

Claim 3, 8, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harari as applied to claim 1, 7 and 1 respectively above, and further in view of Deo.

In reference to claim 3, Harari does not expressly disclose a passcode stored on a smart card and access to user data in the memory device being enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card.

Deo discloses a system where the password is stored on the smart card and permits access to the data only when the password that the user enters matches the password stored on the smart card, column 4 lines 66-67 and column 5 lines 1-2. A password, as defined by the Webster's dictionary, is something that enables one to pass or gain admission. Therefore, the pass code is a type of password. The comparing of the password entered by the user with the password stored in the smart card is a form of authenticating the smart card.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the passcode described by Deo on the smart card described by Harari. One of ordinary skill in the art would have been motivated to do this because the smart cards can perform password verification off-line without connection to a back end computer and are self-validating with the access security code resident thereon, Deo column 2 lines 13-16.

In reference to claim 8, Harari does not expressly disclose a smart card that has a passcode stored on the smart card and is configured to authenticate the user-supplied passcode entered into the computer as a condition for enabling access to the user data.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a password described by Deo on the smart card described by Harari.

One of ordinary skill in the art would have been motivated to do this because the smart cards can perform password verification off-line without connection to a back end computer and are self-validating with the access security code resident thereon, Deo column 2 lines 13-16.

Claim 4 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harari as applied to claim 1 and 7 respectively above, and further in view of Jones et al 5,623,637

In reference to claim 4, Harari does not disclose a memory device that stores a public key and a smart card that stores a corresponding private key and access to the user data in the memory device is enabled upon verification that the public key and the private key are associated.

Jones discloses, in column 9 lines 25-41, a system where a remote host has a public key for encrypting data and a corresponding smart card has the private key for decrypting data. The data would therefore only be accessible to the computer connected to the smart card, if the smart card possesses the correct private key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a private key as in Jones on the smart card described by Harari and a public key as in Jones on the memory device described by Harari so as to enable the verification of the association of the public key and the private key.

One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Art Unit: 2131

In reference to claim 9, Harari does not expressly disclose a public key stored on the memory and a private key stored on the smart card.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a private key as described by Deo on the smart card described by Harari and a public key as described by Deo on the memory described by Harari. One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Claim 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Harari as applied to claim 7 above, and further in view of Deo and Jones.

Harari does not expressly disclose a system where the smart card stores a passcode and a private key of a public/private key pair, with a data memory that stores a public key of the public/private key pair.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

Art Unit: 2131

Jones teaches of a remote device with a public key (the second key) and a local device connected to a smart card that contains the private key (the first key), column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied. Therefore, access is allowed only if the keys are corresponding keys.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the pass code, described by Deo, and private key (the first key), described by Jones on the smart card described by Harari and to store the public key (the second key) on the memory device described by Harari.

One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Harari and Hayes as applied to claim 11 above, and further in view of Deo and Jones.

Harari does not expressly disclose a system where the IC card (smart card) stores a passcode and a private key of a public/private key pair, with a data memory that stores a public key of the public/private key pair.

Deo discloses a password stored on an IC card (smart card), in column 2 lines 66-67 and column 5 lines 1-2.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be

Art Unit: 2131

equivalent to the smart card and the remote device would be equivalent to the memory device.

The user data is only made accessible when the correct private key and public key pair are applied.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the pass code, described by Deo, and private key, described by Jones, on the smart card, described by Harari, and to store the public key on the memory device, described by Harari.

One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Claim 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harari in view of Jones, Deo, and Hayes.

In reference to claim 5, Harari discloses a system comprising of a smart card and a memory device (column 8 lines 24-57). Harari also discloses a system where the smart card is configured to permit use of the private key following validation of a user-entered passcode (column 13 lines 63 to column 14 line 30). Harari further discloses a user profile and a public key stored on the memory device (column 14 lines 5-15). Harari discloses the memory device and the smart card being interface with a common computing unit (Fig. 1).

Harari does not disclose a system where the smart card stores a passcode and a private key from a private/public key pair. Harari does not expressly disclose authentication of a public

Art Unit: 2131

key stored on the memory device using the private key and then permitting access to the user data only on the successful authentication of the public key.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied. In addition, Jones teaches the smart card and the memory device interfacing with a common computer, fig 2 (The smart card is an integral part of the memory device).

Hayes discloses a user profile that is stored on a computer.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the passcode, described by Deo, and the private key, described by Jones, on the smart card, described by Harari, to store the user profile and the public key on the computer hard drive, to interface the smart card and the memory device with a common computer, authentication of a public key stored in the memory device before accessing the user data. One of ordinary skill in the art would have been motivated to do this because when the passcode is stored on the smart card the card can perform password verification off-line without connection to a back end computer and smart cards are self-validating with access security code resident thereon, Deo column 2 lines 13-16. Storing the private key on the smart card and the public key on the memory device increases security of the memory device, Jones column 9 lines 55-60.

In reference to claim 6, Harari discloses a system comprising of a smart card and a memory device (column 8 lines 24-57). Harari also discloses a system where the smart card is configured to permit use of the private key following validation of a user-entered passcode (column 13 line 63 to column 14 line 30). Harari also discloses a system with a smart card reader and a hard drive. The hard drive is interfaced with the computer and the smart card is interfaced with the computer via the smart card reader. Harari discloses the memory device and the smart card being interface with a common computing unit (Fig. 1)

Harari does not disclose a system where the smart card stores a passcode and a private key from a private/public key pair. Harari further does not disclose a user profile and a public key stored on the memory device. Harari does not expressly disclose authentication of a public key stored on the memory device using the private key and then permitting access to the user data only on the successful authentication of the public key.

Deo discloses a password stored on a smart card, in column 2 lines 66-67 and column 5 lines 1-2.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied. In addition, Jones teaches the smart card and the memory device interfacing with a common computer, fig 2 (The smart card is an integral part of the memory device).

Hayes discloses a user profile that is stored on a computer.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the passcode and the private key on the smart card, to store the user profile and the public key on the computer hard drive, to interface the smart card and the memory device with a common computer, authentication of a public key stored in the memory device before accessing the user data. One of ordinary skill in the art would have been motivated to do this because the smart card with password, security system prevents access of unauthorized users while enabling the authorized user quick access data, Deo column 3 lines 4-6, where the data stored in this case would be the user profile. It would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Harari and Hayes in view of Deo.

Harari and Hayes disclose a computer system as applied to claim 11.

Harari does not expressly disclose an IC card (smart card) that stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user's profile.

Deo discloses a smart card that stores the password and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user's profile, column 2 lines 66-67 and column 5 lines 1-2.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the password in the smart card and configure it to authenticate a user-

Art Unit: 2131

supplied passcode entered into the computer as a condition for enabling access to the user's profile. One of ordinary skill in the art would have been motivated to do this because the security system prevents access of an unauthorized user while enabling the authorized user quick access, Deo column 3 lines 4-6.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Harari and Hayes in view of Jones.

Harari and Hayes disclose a computer system as applied to claim 11.

Neither Harari nor Hayes expressly discloses a public key stored on the memory and a private key stored on the smart card.

Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The local device will be equivalent to the smart card and the remote device would be equivalent to the memory device. The user data is only made accessible when the correct private key and public key pair are applied.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store a private key on the smart card and a public key on the memory. One of ordinary skill in the art would have been motivated to do this because it would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Harari in view of Deo, Jones, Sigbjørnsen et al US 6,266,416 B1, and Kutler.

Harari discloses a system that stores user data in a portable memory device, column 6 lines 43 and 44; a computer that interfaces with a smart card (Fig. 1); a portable memory device that interfaces with the computer (column 6 lines 59-62); user-entered password; and use of the card resident key permitted only after validation of the user entered password (column 13 line 63 to column 14 line 30).

Harari does not expressly disclose a system where the a key is stored on the memory device the corresponding key is stored on the smart card, storing a passcode on the smart card, passing the key from the memory device to the smart card, and authenticating the at the smart card using the card resident key.

Deo discloses password stored on a smart card (column 4 lines 66 and 67, column 5 lines 0 and 1).

Jones discloses a system where a key is stored on a remote device (the memory device) and a corresponding key is stored on the local device (the smart card), column 9 lines 24-42.

Sigbjørnsen teaches of a system where an asymmetric authentication key is transferred to the smart card and decrypted in the smart card to initiate an authentication process in the smart card, column 7 lines 44-49.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art would use the system to store the password and a key on the smart card, store a corresponding key on the memory device, and transmitting the stored key from the memory device to the smart card in order to carryout the authentication.

One of ordinary skill in the art would have been motivated to do this because storing the password and a key on the smart card and a corresponding key on the memory device would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60. Carrying out authentication on the smart card give the users complete portability, user authentication can be carried out across operating systems and multiple computers, Kutler, page 13, paragraph 4.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Harari in view of Hayes, Deo, and Jones.

Harari discloses a system with a smart card secured memory. The system receives a user-supplied password from the computer and enables access to the private key on the smart card upon successful authentication of the user-supplied password (column 13 line 63 to column 14 line 30).

Harari does not expressly disclose the user profile stored on the memory device, a password stored on the smart card, and public key and private keys stored on the smart card and the memory device.

Hayes discloses a system where the user profile is stored in memory for the configuration of the computer, page 1 paragraph 4.

Deo discloses a smart card that has a password stored on the smart card (column 4 lines 66 and 67, column 5 lines 0 and 1).

Jones discloses a system where the public key is stored on remote computer (memory device) and a private key stored in host computer (smart card), column 9 lines 24-42.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user profile on the memory device, store the password on the smart card and store corresponding keys on the smart card and the memory device.

One of ordinary skill in the art would have been motivated to do this because storing the password and a key on the smart card and a corresponding key on the memory device would increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

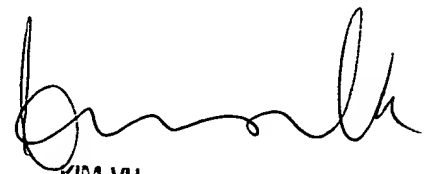
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK
Tuesday, January 06, 2004



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100